UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/856,283	07/24/2001	Lyal Sidney Collins	U-013471-0	6730

26530 7590 10/31/2005

LADAS & PARRY LLP
224 SOUTH MICHIGAN AVENUE
SUITE 1600
CHICAGO, IL 60604

EXAMINER	
GELAGAY, SHEWAYE	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 10/31/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/856,283	COLLINS, LYAL SIDNEY	
	Examiner	Art Unit	
	Shewaye Gelagay	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 August 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4 and 14-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4 and 14-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to Request for Continued Examination filed on August 15, 2005. Claims 1-4 have been amended. Claims 5-13 are cancelled. New claims 14-21 are added. Claims 1-4 and 14-21 are pending.

Response to Arguments

2. Applicant's arguments filled August 15, 2005 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

3. Claim 4 is objected to because of the following informalities: The word "recent" in line 2 should be changed to "recipient". Appropriate correction is required.

Claim 15 is objected to because of the following informalities: Claim 15 recite "apparatus" in the preamble, however, the independent claim 14 in which claim 15 depends on recite "device". Appropriate correction is required.

Claim 16 is objected to because of the following informalities: Claim 16 recite "a computer program product" in the preamble, however, the independent claim 14 in which claim 16 depends on recite "device". Appropriate correction is required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-4 and 14-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mapson WO 98/32260 in view of Schneier et al. (hereinafter Schneier) United States Letter Patent Number 5,956,404.

As per claims 1, 14 and 17:

Mapson teaches a method, a system and a computer program product for securely encoding and transmitting a message by an originating device to one of a-plurality of recipient devices said message being associated with a particular one of a plurality of applications running on the originating device, the method comprising the steps of:

(a) determining a device identifier for the originating device, and an application identifier for each of the plurality of applications thereby forming a plurality of device-identifier/application identifier pairs; (Page 2, line 4; having a first unique identifier; Page 7, lines 13-14; ... with a unique identifier for the secure device and for the transaction)

(b) associating a secret value with each device-identifier/application-identifier pair; (Page 7, lines 12-14; the secure message ... with a unique identifier for the secure device and for the transaction as well as the usual PIN)

In addition, Mapson further disclose a secure message with a unique identifier for the secure device and for the transaction as well as the usual PIN (Page 7, lines 12-14)

and a secure device capable of encrypting multiple data blocks with a stored protected asymmetric key. (Page 5, lines 25-28)

Mapson does not explicitly disclose (c) wherein each said secret value is known to the originating device and to one of the recipient devices; (d) generating a message value by a first process, using the device identifier a particular application identifier and an application value, said application value indexing said message; (e) combining the message value with said secret value associated with the particular application identifier to establish a corresponding secret message value; (f) applying secret message value and the message to an encoding process to form a secure message block; (g) combining the device identifier, the application identifier, the application value and the secure message block, to form a secure message for transmission, said secure message being decodable, dependent upon the device, identifier, the particular application identifier and the application value which are outside the received secure message block by said recipient device to which said secret value associated with particular application identifier is known, said recipient device thereby recovering the message, the device identifier, the particular application identifier and the application value.

Shenier in analogous art, however, discloses a method (c) wherein each said secret value is known to the originating device and to one of the recipient devices; (Figure 3, item 279; Col. 4, lines key ID bits, which identify the private key encrypting the signature package) (d) generating a message value by a first process, using the device identifier a particular application identifier and an application value, said

application value indexing said message; (Col. 3, lines 41-Col. 4, lines 26) (e) combining the message value with said secret value associated with the particular application identifier to establish a corresponding secret message value; (Figure 2; Col. 5, line 35 - Col. 4, line 26) (f) applying secret message value and the message to an encoding process to form a secure message block; (Abstract; Col. 3, lines 51-54; Col. 5, lines 13-16) (g) combining the device identifier, the application identifier, the application value and the secure message block, to form a secure message for transmission, said secure message being decodable, dependent upon the device, identifier, the particular application identifier and the application value which are outside the received secure message block by said recipient device to which said secret value associated with particular application identifier is known, said recipient device thereby recovering the message, the device identifier, the particular application identifier and the application value. (Abstract; Col. 3, lines 51-54; Col. 5, lines 54-13)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Mapson as suggested by, Schenier (Col. 3, lines 12-34) in order to establish an audit trail of actions between the various parties for auditing electronic commerce.

As per claim 2:

The combination of Mapson and Schenier teach all the subject matter as discussed above. In addition, Schenier teaches a method wherein an association of the device identifier, the application identifier, and the application value substantially uniquely identifies the originating device and a purpose of one or more of the message

and the application, and establishes an identifier for the message, said message identifier being bound with the message content by virtue of the encoding process. (Abstract; Col. 3, lines 41-Col. 4, lines 26; Col. 5, lines 13-16)

As per claims 3, 15 and 16:

The combination of Mapson and Schenier teach all the subject matter as discussed above. In addition, Schenier teaches a method, a system and a computer program product wherein the encoding process in step (f) comprises one or more of:

a symmetric encryption process; (Col. 6, lines 1-2)

an integrity process using one of keyed hash and symmetric encryption techniques; (Col. 6, line 4)

a process including both symmetric encryption and keyed integrity; and

including the secret message value in a higher level messaging protocol.

As per claims 4, 18 and 19:

Mapson teach a method, a system and a computer program product for reception of a securely transmitted message by a recipient device, the recipient device being one of a plurality of recipient devices adapted to receive a message from an originating device, said message being associated with a particular one of a plurality of applications running on the originating device, the method comprising the steps of:

(i) extracting one or more of a device identifier, an application identifier and an application value from a received secure message having secure message block, said one or more of the device identifier, the application identifier, and the application value being outside the secure message block; (Page 2, lines 9-11; receiving means is

enabled to decrypt the message using first unique identifier, and includes a list of possible second identifiers for the transmitting means associated with first identifiers)

(j) generating by a first process using the device identifier, the application identifier and the application value a message value; (Page 2, line 4; having a first unique identifier; Page 7, lines 13-14; ... with a unique identifier for the secure device and for the transaction; Page 5, lines 20-21; an advanced transaction number is assigned this may be simply 1,2, etc.; *The office has interpreted application value as an advanced transaction number: The interpretation is given based on the definition of the application value given on the disclosure*)

(k) generating, according to a second process using the device identifier and the application identifier a secret values; (Page 2, lines 26-30; the receiving means stores decryption information associated with the transmitting means ... this provides a unique key for each message without necessity for a real time link)

(l) combining the message value with the secret values, to establish a secret message value; (Page7, lines 12-14; the secure message ... with a unique identifier for the secure device and for the transaction as well as the usual PIN)

(m) extracting a secure message block from the received secure message; and (Page 2, lines 12-13; ...said message block is recognized as valid...)

(n) applying the secret message value and the secure message block to a decoding process to form the securely transmitted message, this message having been securely transmitted by the originating device. (Page 2, lines 26-28; the receiving

means stores decryption information associated with the transmitting means, so that given the first unique identifier and the random number message can be decrypted)

Mapson does not explicitly disclose said one or more of the device identifier, the application identifier, and the application value being outside the secure message block, said application value indexing said message; and a secret values known only to the originating device and the recipient device.

Schenier in analogous art, however, discloses generating a digital signature using private key of the sender of the message through hashing the message and encrypting the hashed message by the private key. (Col. 3, lines 51-54) Schenier further discloses a signature packet that includes message bits, auditing bits and redundancy bits. (Figures 3 and 4). The audit bits, which are outside the message bits, include a device id, key id (a key that identify the private key encrypting the signature package; Col. 4, lines 6-7), packet sequence number (application id) and time-stamp (application value). The signature-packet version indicates to the receiver how the packet is to be processed. (Col. 3, line 41- Col. 4, lines 26; Col. 5, lines 43-Col. 6, lines 64) Bits generated by hashing the prior signature to provide an audit trail of signature and time-stamp to indicate the time when the signature is generated. (Abstract)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Mapson as suggested by, Schenier (Col. 3, lines 12-34) in order to establish an audit trail of actions between the various parties for auditing electronic commerce.

As per claim 23:

The combination of Mapson and Schenier teach all the subject matter as discussed above. In addition, Schenier teaches a method for reception wherein:

a plurality of applications are running on the recipient device; (Col. 6, lines 40-45) and

the application identifier extracted in the extracting step (i) is used to identify one of the applications running on the recipient device, said identified application being adapted to process the securely transmitted message decoded in step (n). (Abstract; Col. 6, lines 40-64)

As per claim 20:

Mapson teaches a system providing secure communications, the system comprising an originating device and one or more receiving devices, wherein:

(a) determining a device identifier for the originating device, and an application identifier for each of the plurality of applications thereby forming a plurality of device-identifier/application identifier pairs; (Page 2, line 4; Page 7, lines 13-14)

(b) associating a secret value with each device-identifier/application-identifier pair; (Page 7, lines 12-14)

(i) extracting one or more of a device identifier, an application identifier and an application value from a received secure message having secure message block, said one or more of the device identifier, the application identifier, and the application value being outside the secure message block; (Page 2, lines 9-11)

(j) generating by a first process using the device identifier, the application identifier and the application value a message value; (Page 2, line 4; Page 7, lines 13-14)

(k) generating, according to a second process using the device identifier and the application identifier a secret values; (Page 2, lines 26-30)

(l) combining the message value with the secret values, to establish a secret message value; (Page7, lines 12-14)

(m) extracting a secure message block from the received secure message; and (Page 2, lines 12-13)

(n) applying the secret message value and the secure message block to a decoding process to form the securely transmitted message, this message having been securely transmitted by the originating device. (Page 2, lines 26-28)

In addition, Mapson further disclose a secure message with a unique identifier for the secure device and for the transaction as well as the usual PIN (Page 7, lines 12-14) and a secure device capable of encrypting multiple data blocks with a stored protected asymmetric key. (Page 5, lines 25-28)

Mapson does not explicitly disclose (c) wherein each said secret value is known to the originating device and to one of the recipient devices; (d) generating a message value by a first process, using the device identifier a particular application identifier and an application value, said application value indexing said message; (e) combining the message value with said secret value associated with the particular application identifier to establish a corresponding secret message value; (f) applying secret message value

and the message to an encoding process to form a secure message block; (g) combining the device identifier, the application identifier, the application value and the secure message block, to form a secure message for transmission, said secure message being decodable, dependent upon the device, identifier, the particular application identifier and the application value which are outside the received secure message block by said recipient device to which said secret value associated with particular application identifier is known, said recipient device thereby recovering the message, the device identifier, the particular application identifier and the application value.

Shenier in analogous art, however, discloses a method (c) wherein each said secret value is known to the originating device and to one of the recipient devices; (Figure 3, item 279; Col. 4, lines key ID bits, which identify the private key encrypting the signature package) (d) generating a message value by a first process, using the device identifier a particular application identifier and an application value, said application value indexing said message; (Col. 3, lines 41-Col. 4, lines 26) (e) combining the message value with said secret value associated with the particular application identifier to establish a corresponding secret message value; (Figure 2; Col. 5, line 35 - Col. 4, line 26) (f) applying secret message value and the message to an encoding process to form a secure message block; (Abstract; Col. 3, lines 51-54; Col. 5, lines 13-16) (g) combining the device identifier, the application identifier, the application value and the secure message block, to form a secure message for transmission, said secure message being decodable, dependent upon the device, identifier, the particular

application identifier and the application value which are outside the received secure message block by said recipient device to which said secret value associated with particular application identifier is known, said recipient device thereby recovering the message, the device identifier, the particular application identifier and the application value. (Abstract; Col. 3, lines 51-54; Col. 5, lines 54-13)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Mapson as suggested by, Schenier (Col. 3, lines 12-34) in order to establish an audit trail of actions between the various parties for auditing electronic commerce.

As per claim 21:

The combination of Mapson and Schenier teach all the subject matter as discussed above. In addition, Mapson further disclose a system:

wherein said originating device comprises:

(n) first processing means; (Page 2, lines 6-7)

(o) transmitting means adapted to perform one or more of establishing and maintaining communications with a receiving means, said first processing means being adapted to control said transmitting means, and adapted to support features (a) to (g); (Page 2,lines 4-8)

wherein a said receiving device comprises:

(p) second processing means; (Page 2, lines 26-28) and

(q) the receiving means, being adapted to perform one or more of establishing and maintaining communications in conjunction with said transmitting means, said

second processing means being adapted control said receiving means, and further adapted to support features (e) to (j). (Page 2, lines 9-14)

As per claim 22:

The combination of Mapson and Schenier teach all the subject matter as discussed above. In addition, Mapson further disclose a system wherein said originating device comprises one of:

(r) a PC comprising the transmitting means, a smart card reader, the first processing means being responsive to the smart card reader and adapted to control said transmitting means, said originating device further comprising a smart card adapted to interface with the smart card reader, said smart card having on board second processing means which in conjunction with said first processing means are adapted to support features (a) to (g); and (Page 4, lines 22-24)

(s) a mobile telephone, comprising the transmitting means, the first processing means being adapted to control said transmitting means, and also adapted to support features (a) to (g); and

(t) a set top box, comprising the transmitting means, the first processing means being adapted to control said transmitting means, and also adapted to support features (a) to (g); and

(u) a cable modem, comprising the transmitting means, the first processing means being adapted to control said transmitting means, and also adapted to support features (a) to (g); and

(v) a personal digital assistant, comprising the transmitting means, the first processing means being adapted to control said transmitting means, and also adapted to support features (a) to (g).

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See Form PTO-892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shewaye Gelagay SG
10/24/05

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER